

Capturing and Encoding Unique User Attributes in Media Signals

Related Application Data

The subject matter of the present application is related to that disclosed in US Patent 5,862,260, and in co-pending application 09/503,881, filed February 14, 2000;
5 which are hereby incorporated by reference.

Technical Field

The invention relates to multimedia signal processing, and in particular, relates to encoding information into media signals.

Background and Summary

Advances in electronics have made it trivial to capture and edit creative digital works, including images, audio, and video. These advances also make it difficult to control unauthorized copying and alteration of these works. In particular, one challenge presented by this technology is to uniquely associate a work with its creator. Another
15 challenge is to prevent tampering of the work, or at least provide a reliable method for detecting tampering.

One way to associate multimedia data with its owner or creator is to hide identifying information in the media signal through data hiding or steganography. Steganography refers to a process of hiding information into a signal. One example of
20 steganography is digital watermarking. Digital watermarking is a process for modifying media content to embed a machine-readable code into the data content. The data may be modified such that the embedded code is imperceptible or nearly imperceptible to the user, yet may be detected through an automated detection process. Most commonly, digital watermarking is applied to media such as images, audio signals, and video signals.
25 However, it may also be applied to other types of data, including documents (e.g.,

through line, word or character shifting), software, multi-dimensional graphics models, and surface textures of objects.

Digital watermarking systems have two primary components: an embedding component that embeds the watermark in the media content, and a reading component that detects and reads the embedded watermark. The embedding component embeds a watermark by altering data samples of the media content in the spatial, temporal or some other transform domain (e.g., Fourier, Discrete Cosine, Wavelet Transform domains). The reading component analyzes target content to detect whether a watermark is present. In applications where the watermark encodes information (e.g., a message), the reader extracts this information from the detected watermark.

The present assignee's work in steganography, data hiding and watermarking is reflected in U.S. Patent 5,862,260; in copending applications 09/503,881 and 09/452,023; and in published specifications WO 9953428 and WO0007356 (corresponding to US 09/074,034 and 09/127,502). A great many other approaches are familiar to those skilled in the art. The artisan is presumed to be familiar with the full range of literature about steganography, data hiding and watermarking.

The invention provides methods, systems and devices for capturing and encoding a user attribute in a media signal. It also provides methods, systems and devices for authenticating the media signal using the encoded user attribute data.

One aspect of the invention is a method for capturing and encoding a user attribute in a media signal. This method applies to a variety of media signals, including images (still and video) and audio. The method captures a user attribute of the user of a media signal capture device, such as a camera, video recorder, etc. It then encodes the user attribute into a media signal captured by the device. The method may be implemented in the media signal capture device, which enables the user attribute data to be captured from the user and encoded into content as it is being captured by the device.

One type of user attribute data is a retinal scan. This type of data is particularly suited for digital camera applications. In such applications, an image sensor may capture the photographer's retinal image for immediate encoding into an image captured with the

same or a different image sensor in the camera. The method applies to other media capture devices, media signal types, and user attributes such as a voice signature, fingerprint, etc.

Another aspect of the invention is a media signal capture device capable of
5 encoding a user attribute in a media signal captured in the device. The device includes a user attribute capture unit for capturing a user attribute of a user of the media signal capture device. It also includes an encoder for encoding the user attribute into a media signal captured by the device.

Another aspect of the invention is a method of authenticating a media signal. The
10 method decodes user attribute data encoded in the media signal within a media signal capture device that captured the media signal. It then compares the decoded user attribute data with user attribute data computed for a person. This process may be used to verify that a creator of the content, such as photographer, did create the media content in question (e.g., a photograph, video recording, etc.).

15 Further features will become apparent with reference to the following detailed description and accompanying drawings.

Brief Description of the Drawings

Fig. 1 is a diagram illustrating a method for encoding an attribute of a user of a
20 media capture device into a media signal captured by the device.

Fig. 2 is a diagram illustrating a method for encoding retinal scan data into an image.

Fig. 3 illustrates a method for evaluating an image processed as shown in Fig. 2.

25 Detailed Description

Fig. 1 is a diagram illustrating a method for encoding a user attribute of a user of a media capture device into a media signal captured by the device. This method integrates a process of capturing the media signal (e.g., image or audio signal) with a process of

encoding a user attribute into the media signal. By combining these processes, it provides a convenient and reliable way of encoding information about the content creator into the content. Additionally, since it can be performed at the time of capture of the content, it enables subsequent alteration of the content to be detected. These features
5 make the method particularly useful in associating the content with its creator and authenticating the content.

As depicted in Fig. 1, the method captures a user attribute (100) of the user of the device (102). Preferably, the user attribute should uniquely identify the user, should enable immediate and automated capture by the device, and should allow capture at or
10 near the time of capture of the media signal in which it is embedded. However, these criteria are not absolute necessities for all applications. One example of a user attribute is an image of an identifying characteristic of the user such as a retinal scan or fingerprint. Another is a voice recording. The capture of this data is implemented in a user attribute capture unit, which may include an image sensor and optical elements, a digital recorder
15 and user input controls, a fingerprint scanning element, etc.

After capturing the user attribute, the method may optionally convert it into a more compact data representation. In a typical application, the user attribute is in the form of an electronic signal, such as a digital image of a retinal scan or fingerprint or a digital audio recording of the user's voice. In these cases, the method transforms the
20 signal representing the user attribute into more compact, yet statistically unique user attribute data. Statistically unique, in this context, refers to an attribute that is statistically improbable of being generated from two different users. The process of generating the user attribute data is generally depicted as a hash in Fig. 1 (104). A "hash" in this context refers to transformation in a data representation from one form to another where the data
25 retains statistically unique characteristics.

For additional security, cryptographic functions may be used to digitally sign and encrypt the user attribute data. Encryption provides an additional layer of security to prevent unwanted uses of the encoded information. Some examples of applicable cryptographic methods include RSA, DES, IDEA (International Data Encryption

Algorithm), skipjack, discrete log systems (e.g., El Gamal Cipher), elliptic curve systems, cellular automata, etc.

These cryptographic methods may be used to create a digital signature to place in a watermark message. Public key cryptographic methods employ a private and public
5 key. The private key is kept secret, and the public key is distributed. To digitally sign a user attribute data, the media capture device encrypts the message with a private key. The private key is uniquely associated with the device or a particular user. Those having a public key verify that the message has originated from the holder of the private key by using the public key to decrypt the message.

10 The user attribute data may be both encrypted and digitally signed using two stages of encryption. In the encoding process, a digital signature stage encrypts at least part of the data with a private key. An encryption stage then encrypts the signed data with a public key. The decoding process reverses these steps. First, a decryption stage decrypts the data with a private key corresponding to public key used in the encryption
15 stage. Then, a second stage decrypts the output of the previous stage with the public key corresponding to the private key used to authenticate the data.

As a separate, and potentially concurrent process to the process of capturing the user attribute data, the method captures a media signal (106) into which the user attribute data will be embedded (108). Some examples include capturing an image, or a sequence
20 of video frames in a camera, recording an audio signal, or both image and audio capture (such as in a video camera).

Next, the method encodes the user attribute data into the media signal to create an encoded media signal (110, 112). One way to encode the data is to steganographically embed it in the media signal. Examples of steganographic embedding implementations
25 are provided in US Patent 5,862,260, and U.S. Patent Application No. 09/503,881, filed February 14, 2000, which are incorporated by reference. Another way to encode the user attribute data is to place it in a file header of the media signal.

The method outlined above enables user attributes to be encoded into a media signal at or near the time of capture. For example, the method may be implemented

within media capture devices such as cameras, scanners, recorders, etc. This feature links the user of the capture device and creator of the media content to the content. In cases where steganographic techniques, such as digital watermarking, are used to encode the user attribute data, the association between the user attributes and the content remains
5 through various transformations and file format changes, is imperceptible or substantially imperceptible to humans viewing or listening to the content, and can be used to establish whether or not the content has been tampered with after capture.

To provide an example, Fig. 2 depicts a system and method for encoding retinal scan data into an image. In this example, the method is implemented within a single lens
10 reflex digital camera. This type of configuration is common in commercially available 35mm digital cameras. The single lens reflex body 200 includes an eyepiece 202 through which the photographer view's the subject of the photograph. An optical element 204 directs light reflected from the photographer's eye 206 (Image source 1) to an image
15 sensor 208. The image sensor depicted here is a CCD array. Alternative sensor technology, such as a CMOS sensor may also be used.

Fig. 2 shows a configuration where the sensor used to record a user attribute also captures an image into which the user attribute is encoded. The light from the subject (Image source 2) enters the camera through its primary optical element 210 (e.g., an image field lens) and is directed to the image sensor 208. In response to the user
20 actuating a shutter command (or other analogous signal capture command), the camera time multiplexes the image sensor to capture user attribute data and the subject image. As an alternative, the camera may include a separate image sensors for user attribute and subject image data, respectively. Using separate sensors, the camera can capture the user attribute data at the same time as the subject image data.

25 A controller 212, such as the Central Processing Unit/ Digital Camera (CPU/DCAM) integrated circuit shown in Fig. 2, controls image capture from the two image sources in response to a user's image capture input command. The controller communicates with a memory subsystem 214, which includes one or more memory

devices for storing program code, image data, and image metadata, including user attribute data.

One operation scenario proceeds as depicted in Fig. 2 and described below. First, the photographer presses a shutter command button on the camera (300). In response, the sensor captures an image of the photographer's eye through the eyepiece (302). The controller transfers the image to memory, analyzes it to derive a statistically unique retina image, and hashes the retina image into an identifier to be encoded into an image (304). While a variety of hashing algorithms can be used, the hash algorithm used to compute the identifier should retain the statistically unique characteristic of the retina image.

Examples of hashing algorithms include MD5, MD2, SHA, SHA1.

While it holds this identifier in memory A, the controller captures an image of the subject through the primary optical element 210 and places it into memory B (306). Next, the controller performs conventional color formatting of the captured image, such as raw image to Bayer RGG image formatting (308).

The controller may also gather additional metadata relating to the image. There are many types of metadata such as: a time stamp, camera settings, a user name, location, etc. The controller may encode a cross reference link to this metadata into the image or its file header/footer. The cross reference link may be a number or other code (HTML link, pointer, address, index, etc.) that references a device where the metadata is stored. For example, the metadata may be stored in an external database and referenced via the link. The metadata may be transferred from the camera along with the image data via a wire or wireless link to the database.

Alternatively, the controller may encode the metadata directly into the image or the file header/footer. For example, metadata such as a time stamp, location (e.g., GPS coordinates), etc. may be concatenated with the identifier representing user attribute data and encoded into the image. The metadata is generated by the camera, devices in the camera (a GPS device, clock) or from user input. The embedded metadata may also include a hash of the image that is later used to detect image alteration. To be effective, a hash function used to compute an image hash that is embedded in the image should be

insensitive to the alteration of the image caused by embedding auxiliary data into the image. For more on associating metadata with media signals such as images, audio and video, see co-pending application 09/507,096, entitled Associating Data with Images In Imaging Systems, filed on February 17, 2000.

5 Returning to the example depicted in Fig. 2, the controller embeds the identifier into the formatted image using a watermark encoding process (312). Examples of watermark encoding processes are provided in US Patent 5,862,260, and in co-pending application 09/503,881, filed February 14, 2000; which are hereby incorporated by reference. Other image watermark, steganographic or data hiding programs may be used
10 to encode the identifier in the subject image as well.

Finally, the controller writes the image marked with the identifier to a file (314). The user or controller may transfer the image from the camera to another device via a portable memory device (such as flash memory, floppy disk, etc.) or a wire or wireless communication link (e.g., infrared, radio, wireless modem, modem, USB, USB2, IEEE
15 1394, computer network connection, etc.). As an additional step, the controller may also hash the marked image and insert the image hash in the file header/footer before transferring it. One simple hash is a check sum. Other cryptographic hashes may be used, such as those cited earlier.

Fig. 3 illustrates a method for evaluating an image processed as shown in Fig. 2.
20 In cases where the image file includes an image hash, the process begins by evaluating the hash to determine whether the image has been altered. The input is a suspect image 400, which may have undergone some tampering or alteration after being captured. The method reads the image hash from the file (402) (e.g., from the header or footer), re-computes the image hash for the suspect image (404), and compares this computed hash
25 with the one read from the file (406). If the two hashes differ, then the image has been altered.

Next, the method proceeds to check the user attribute data. It decodes the embedded user attribute data (408, 410) from the image using a decoder compatible with

the encoder. It then compares the extracted user data with separately computed user data to determine whether there is a match (412).

There are several application scenarios for this user authentication process. In one scenario, the user attribute data for a person purported to be the photographer is captured (414, 416), hashed (418, 420) and compared with the extracted user data (412). If there is a match, then the photographer is deemed to have created the suspect image. In another scenario, user attributes (416) for several photographers are captured (416), hashed (418), and stored in a database (420), along with information about the person. The user attribute data extracted from the image is used as an index to this database to look up the identity of the photographer.

The processes depicted in Fig. 3 may be implemented in hardware, software or a combination of hardware and software. For example, the process may be incorporated into an authentication system implemented in a computer or computer network. The processes depicted in Fig. 3 may be implemented in programs executed from the system's memory (a computer readable medium, such as an electronic, optical or magnetic storage device.) Suspect media signals may be delivered to the computer electronically via a wire or wireless network or memory device (e.g., flash memory, optical disk, magnetic storage device, etc.), or by scanning or recording an analog form of the suspect media signal (scanning a photograph, or recording suspect analog audio signals). In the case where analog versions of the suspect signal are evaluated, steganographic embedding processes used to encode the user attribute data should be selected to survive digital to analog and analog to digital conversion.

While the specific examples provided in Figs. 2 and 3 related to digital cameras, similar processes may be implemented in other media signal capture devices, including scanners, and audio and video recorders. Retinal scan data is one example of a user attribute data. Other types of user attribute data include a fingerprint or voice signature. A fingerprint may be captured by requesting the user of the capture device to place a finger on a scanning element, and then taking an image of the finger. A voice signature may be captured by recording the user's voice, and then coding a digital recording of the

voice into signature for embedding in the media signal. One way to encode the digital recording is to use audio compression, and particularly, coding designed for voice signals.

Concluding Remarks

5 Having described and illustrated the principles of the technology with reference to specific implementations, it will be recognized that the technology can be implemented in many other, different, forms. To provide a comprehensive disclosure without unduly lengthening the specification, applicants incorporate by reference the patents and patent applications referenced above. These patents and patent applications provide additional
10 details about implementing watermarking systems.

 The particular combinations of elements and features in the above-detailed embodiments are exemplary only; the interchanging and substitution of these teachings with other teachings in this and the incorporated-by-reference patents/applications are also contemplated.

15